A discrete form of the theorem that each field endomorphism of $\mathbb{R}$ ($\mathbb{Q}_p$) is the identity

Apoloniusz Tyszka

Summary. Let $\boldsymbol{K}$ be a field and $\boldsymbol{F}$ denote the prime field in $\boldsymbol{K}$. Let $\widetilde{\boldsymbol{K}}$ denote the set of all $r \in \boldsymbol{K}$ for which there exists a finite set $A(r)$ with $\{r\} \subseteq A(r) \subseteq \boldsymbol{K}$ such that each mapping $f : A(r) \to \boldsymbol{K}$ that satisfies: if $1 \in A(r)$ then $f(1) = 1$, if $a, b \in A(r)$ and $a + b \in A(r)$ then $f(a+b) = f(a) + f(b)$, if $a, b \in A(r)$ and $a \cdot b \in A(r)$ then $f(a \cdot b) = f(a) \cdot f(b)$, satisfies also $f(r) = r$. Obviously, each field endomorphism of $\boldsymbol{K}$ is the identity on $\widetilde{\boldsymbol{K}}$. We prove: $\widetilde{\boldsymbol{K}}$ is a countable subfield of $\boldsymbol{K}$, if $\mathrm{char}(\boldsymbol{K}) \neq 0$ then $\widetilde{\boldsymbol{K}} = \boldsymbol{F}$, $\widetilde{\mathbb{C}} = \mathbb{Q}$, if each element of $\boldsymbol{K}$ is algebraic over $\boldsymbol{F} = \mathbb{Q}$ then $\widetilde{\boldsymbol{K}} = \{x \in \boldsymbol{K} : x \text{ is fixed for all automorphisms of } \boldsymbol{K}\}$, $\widetilde{\mathbb{R}}$ is equal to the field of real algebraic numbers, $\widetilde{\mathbb{Q}_p}$ is equal to the field $\{x \in \mathbb{Q}_p : x \text{ is algebraic over } \mathbb{Q}\}$.

Let $\boldsymbol{K}$ be a field and $\boldsymbol{F}$ denote the prime field in $\boldsymbol{K}$. Let $\widetilde{\boldsymbol{K}}$ denote the set of all $r \in \boldsymbol{K}$ for which there exists a finite set $A(r)$ with $\{r\} \subseteq A(r) \subseteq \boldsymbol{K}$ such that each mapping $f : A(r) \to \boldsymbol{K}$ that satisfies:

(1) if $1 \in A(r)$ then $f(1) = 1$,
(2) if $a, b \in A(r)$ and $a + b \in A(r)$ then $f(a+b) = f(a) + f(b)$,
(3) if $a, b \in A(r)$ and $a \cdot b \in A(r)$ then $f(a \cdot b) = f(a) \cdot f(b)$,

satisfies also $f(r) = r$. In this situation we say that $A(r)$ is adequate for r. Obviously, if $f : A(r) \to \boldsymbol{K}$ satisfies condition **(2)** and $0 \in A(r)$, then $f(0) = 0$. If $A(r)$ is adequate for r and $A(r) \subseteq B \subseteq \boldsymbol{K}$, then B is adequate for r. We have:

$$\textbf{(4)} \qquad \widetilde{\boldsymbol{K}} \subseteq \widehat{\boldsymbol{K}} := \bigcap_{\sigma \in \mathrm{End}(\boldsymbol{K})} \{x \in \boldsymbol{K} : \sigma(x) = x\} \subseteq \boldsymbol{K},$$

$\widehat{\boldsymbol{K}}$ is a field. Let $\widetilde{\boldsymbol{K}}_n$ ($n = 1, 2, 3, ...$) denote the set of all $r \in \boldsymbol{K}$ for which there exists $A(r)$ with $\{r\} \subseteq A(r) \subseteq \boldsymbol{K}$ such that $\mathrm{card}(A(r)) \leq n$ and $A(r)$ is adequate for r. Obviously,

$$\widetilde{\boldsymbol{K}}_1 \subseteq \widetilde{\boldsymbol{K}}_2 \subseteq \widetilde{\boldsymbol{K}}_3 \subseteq ... \subseteq \widetilde{\boldsymbol{K}} = \bigcup_{n=1}^{\infty} \widetilde{\boldsymbol{K}}_n.$$

Theorem 1. $\widetilde{\boldsymbol{K}}$ is a subfield of $\boldsymbol{K}$.

Proof. We set $A(0) = \{0\}$ and $A(1) = \{1\}$, so $0, 1 \in \widetilde{\boldsymbol{K}}$. If $r \in \widetilde{\boldsymbol{K}}$ then $-r \in \widetilde{\boldsymbol{K}}$, to see it we set $A(-r) = \{0, -r\} \cup A(r)$. If $r \in \widetilde{\boldsymbol{K}} \setminus \{0\}$ then $r^{-1} \in \widetilde{\boldsymbol{K}}$, to see it we set $A(r^{-1}) = \{1, r^{-1}\} \cup A(r)$. If $r_1, r_2 \in \widetilde{\boldsymbol{K}}$ then $r_1 + r_2 \in \widetilde{\boldsymbol{K}}$, to see it we set $A(r_1 + r_2) = \{r_1 + r_2\} \cup A(r_1) \cup A(r_2)$. If $r_1, r_2 \in \widetilde{\boldsymbol{K}}$ then $r_1 \cdot r_2 \in \widetilde{\boldsymbol{K}}$, to see it we set $A(r_1 \cdot r_2) = \{r_1 \cdot r_2\} \cup A(r_1) \cup A(r_2)$.

2000 Mathematics Subject Classification. Primary: 12E99, 12L12.
Key words and phrases: field endomorphism, field endomorphism of $\mathbb{Q}_p$, field endomorphism of $\mathbb{R}$, p-adic number that is algebraic over $\mathbb{Q}$, real algebraic number.

Corollary 1. If $\mathrm{char}(\boldsymbol{K}) \neq 0$ then $\widetilde{\boldsymbol{K}} = \widehat{\boldsymbol{K}} = \boldsymbol{F}$.

Proof. Let $\mathrm{char}(\boldsymbol{K}) = p$. The Frobenius homomorphism $\boldsymbol{K} \ni x \to x^p \in \boldsymbol{K}$ moves all $x \in \boldsymbol{K} \setminus \boldsymbol{F}$. It gives $\widehat{\boldsymbol{K}} = \boldsymbol{F}$, so by **(4)** and Theorem 1 $\widetilde{\boldsymbol{K}} = \widehat{\boldsymbol{K}} = \boldsymbol{F}$.

Corollary 2. $\widetilde{\mathbb{C}} = \widehat{\mathbb{C}} = \mathbb{Q}$.

Proof. The author proved ([20]) that for each $r \in \mathbb{C} \setminus \mathbb{Q}$ there exists a field automorphism $f : \mathbb{C} \to \mathbb{C}$ such that $f(r) \neq r$. By this and **(4)** $\widetilde{\mathbb{C}} \subseteq \widehat{\mathbb{C}} \subseteq \mathbb{Q}$, so by Theorem 1 $\widetilde{\mathbb{C}} = \widehat{\mathbb{C}} = \mathbb{Q}$.

Theorem 2. For each $n \in \{1, 2, 3, ...\}$ $\mathrm{card}(\widetilde{\boldsymbol{K}}_n) \leq (n+1)^{n^2+n+1}$, $\widetilde{\boldsymbol{K}}$ is countable.

Proof. If $\mathrm{card}(\boldsymbol{K}) < n$ then $\mathrm{card}(\widetilde{\boldsymbol{K}}_n) \leq \mathrm{card}(\boldsymbol{K}) < n < (n+1)^{n^2+n+1}$. In the rest of the proof we assume that $\mathrm{card}(\boldsymbol{K}) \geq n$. Let $r \in \widetilde{\boldsymbol{K}}_n$ and some $A(r) = \{r = x_1, ..., x_n\}$ is adequate for r. Let also $x_i \neq x_j$ if $i \neq j$. We choose all formulae $x_i = 1$ $(1 \leq i \leq n)$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$ $(1 \leq i \leq j \leq n,\ 1 \leq k \leq n)$ that are satisfied in $A(r)$. Joining these formulae with conjunctions we get some formula Φ. Let V denote the set of variables in Φ, $x_1 \in V$ since otherwise for any $s \in \boldsymbol{K} \setminus \{r\}$ the mapping $f = \mathrm{id}(A(r) \setminus \{r\}) \cup \{(r, s)\}$ satisfies conditions **(1)**-**(3)** and $f(r) \neq r$. The formula $\underbrace{...\ \exists x_i\ ...}_{x_i \in V,\ i \neq 1} \quad \Phi$ is satisfied in $\boldsymbol{K}$ if and only if $x_1 = r$. There are $n+1$ possibilities:

$$1 = x_1, \quad ..., \quad 1 = x_n, \quad 1 \notin \{x_1, ..., x_n\}.$$

For each $(i, j) \in \{(i, j) : 1 \leq i \leq j \leq n\}$ there are $n+1$ possibilities:

$$x_i + x_j = x_1, \quad ..., \quad x_i + x_j = x_n, \quad x_i + x_j \notin \{x_1, ..., x_n\}.$$

For each $(i, j) \in \{(i, j) : 1 \leq i \leq j \leq n\}$ there are $n+1$ possibilities:

$$x_i \cdot x_j = x_1, \quad ..., \quad x_i \cdot x_j = x_n, \quad x_i \cdot x_j \notin \{x_1, ..., x_n\}.$$

Since $\mathrm{card}(\{(i, j) : 1 \leq i \leq j \leq n\}) = \frac{n^2+n}{2}$ the number of possible formulae Φ does not exceed $(n+1) \cdot (n+1)^{\frac{n^2+n}{2}} \cdot (n+1)^{\frac{n^2+n}{2}} = (n+1)^{n^2+n+1}$. Thus $\mathrm{card}(\widetilde{\boldsymbol{K}}_n) \leq (n+1)^{n^2+n+1}$, so $\widetilde{\boldsymbol{K}} = \bigcup_{n=1}^{\infty} \widetilde{\boldsymbol{K}}_n$ is countable.

Remark 1. For any field $\boldsymbol{K}$ the field $\widetilde{\boldsymbol{K}}$ is equal to the subfield of all $x \in \boldsymbol{K}$ for which $\{x\}$ is existentially $\emptyset$-definable in $\boldsymbol{K}$. This gives an alternative proof of Theorems 6 and 7.

Let a field $\boldsymbol{K}$ extends $\mathbb{Q}$ and each element of $\boldsymbol{K}$ is algebraic over $\mathbb{Q}$. R. M. Robinson proved ([17]): if $r \in \boldsymbol{K}$ is fixed for all automorphisms of $\boldsymbol{K}$, then there exist $U(y), V(y) \in \mathbb{Q}[y]$ such that $\{r\}$ is definable in $\boldsymbol{K}$ by the formula $\exists y\ (U(y) = 0 \wedge x = V(y))$. Robinson's theorem implies the next theorem.

Theorem 3. If a field $\boldsymbol{K}$ extends $\mathbb{Q}$ and each element of $\boldsymbol{K}$ is algebraic over $\mathbb{Q}$, then $\widetilde{\boldsymbol{K}} = \{x \in \boldsymbol{K} : x \text{ is fixed for all automorphisms of } \boldsymbol{K}\}$.

We use below "bar" to denote the algebraic closure of a field.

Theorem 4 ([21]). If $\boldsymbol{K}$ is a field and some subfield of $\boldsymbol{K}$ is algebraically closed, then $\widetilde{\boldsymbol{K}}$ is the prime field in $\boldsymbol{K}$.

Theorem 5. If a field $\boldsymbol{K}$ extends $\mathbb{Q}$ and $r \in \widetilde{\boldsymbol{K}}$, then $\{r\}$ is definable in $\boldsymbol{K}$ by a formula of the form $\exists x_1 ... \exists x_m T(x, x_1, ..., x_m) = 0$, where $m \in \{1, 2, 3, ...\}$ and $T(x, x_1, ..., x_m) \in \mathbb{Q}[x, x_1, ..., x_m]$.

Proof. From the definition of $\widetilde{\boldsymbol{K}}$ it follows that $\{r\}$ is definable in $\boldsymbol{K}$ by a finite system **(S)** of polynomial equations of the form $x_i + x_j - x_k = 0$, $x_i \cdot x_j - x_k = 0$, $x_i - 1 = 0$, cf. the proof of Theorem 2. If $\overline{\mathbb{Q}} \subseteq \boldsymbol{K}$, then by Theorem 4 each element of $\widetilde{\boldsymbol{K}}$ is definable in $\boldsymbol{K}$ by a single equation $x - w = 0$, where $w \in \mathbb{Q}$. If $\overline{\mathbb{Q}} \not\subseteq \boldsymbol{K}$, then there exists a polynomial

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \in \mathbb{Q}[x] \quad (n \geq 2,\ a_n \neq 0)$$

having no root in $\boldsymbol{K}$. By this, the polynomial

$$B(x, y) := a_n x^n + a_{n-1} x^{n-1} y + ... + a_1 x y^{n-1} + a_0 y^n$$

satisfies

$$\forall u, v \in \boldsymbol{K}\ ((u = 0 \land v = 0) \Longleftrightarrow B(u, v) = 0)\,, \tag{5}$$

see [5]. Applying **(5)** to **(S)** we obtain that **(S)** is equivalent to a single polynomial equation.

1. A discrete form of the theorem that each field endomorphism of $\mathbb{R}$ is the identity

Let $\mathbb{R}^{\rm alg}$ denote the field of real algebraic numbers.

Theorem 6. $\widetilde{\mathbb{R}} = \mathbb{R}^{\rm alg}$.

Proof. We prove:

(6) if $r \in \mathbb{R}^{\rm alg}$ then $r \in \widetilde{\mathbb{R}}$.

We present three proofs of **(6)**.

(I). Let $r \in \mathbb{R}$ be an algebraic number of degree n. Thus there exist integers $a_0, a_1, ..., a_n$ satisfying

$$a_n r^n + ... + a_1 r + a_0 = 0$$

and $a_n \neq 0$. We choose $\alpha, \beta \in \mathbb{Q}$ such that $\alpha < r < \beta$ and the polynomial

$$a_n x^n + ... + a_1 x + a_0$$

has no roots in $[\alpha, \beta]$ except r. Let $\alpha = \frac{k_1}{k_2}$, $\beta = \frac{l_1}{l_2}$, where $k_1, l_1 \in \mathbb{Z}$ and $k_2, l_2 \in \mathbb{Z} \setminus \{0\}$. We put $a = \max\{|a_0|, |a_1|, ..., |a_n|, |k_1|, |k_2|, |l_1|, |l_2|\}$. Then

$$A(r) = \{\sum_{i=0}^{n} b_i r^i : b_i \in \mathbb{Z} \cap [-a, a]\} \cup \{\alpha, r - \alpha, \sqrt{r - \alpha}, \beta, \beta - r, \sqrt{\beta - r}\}$$

is adequate for r. Indeed, if $f : A(r) \to \mathbb{R}$ satisfies conditions **(1)**-**(3)** then

$$a_n f(r)^n + ... + a_1 f(r) + a_0 = f(a_n r^n + ... + a_1 r + a_0) = f(0) = 0,$$

so $f(r)$ is a root of $a_n x^n + ... + a_1 x + a_0$. Moreover,

$$f(r) - \alpha = f(r) - f(\alpha) = f(r - \alpha) = f((\sqrt{r - \alpha})^2) = (f(\sqrt{r - \alpha}))^2 \geq 0$$

and

$$\beta - f(r) = f(\beta) - f(r) = f(\beta - r) = f((\sqrt{\beta - r})^2) = (f(\sqrt{\beta - r}))^2 \geq 0.$$

Therefore, $f(r) = r$.

(II) (sketch). Let $T(x) \in \mathbb{Q}[x] \setminus \{0\}$, $T(r) = 0$. We choose $\alpha, \beta \in \mathbb{Q}$ such that $\alpha < r < \beta$ and $T(x)$ has no roots in $[\alpha, \beta]$ except r. Then the polynomial

$$(1 + x^2)^{\deg(T(x))} \cdot T\left(\alpha + \frac{\beta - \alpha}{1 + x^2}\right) \in \mathbb{Q}[x]$$

has exactly two real roots: x_0 and $-x_0$. Thus $x_0^2 \in \widetilde{\mathbb{R}}$. By Theorem 1 $\widetilde{\mathbb{R}}$ is a field, so $\mathbb{Q} \subseteq \widetilde{\mathbb{R}}$. Therefore, $r = \alpha + \frac{\beta - \alpha}{1 + x_0^2} \in \widetilde{\mathbb{R}}$.

(III). The classical Beckman-Quarles theorem states that each unit-distance preserving mapping from $\mathbb{R}^n$ to $\mathbb{R}^n$ ($n \geq 2$) is an isometry ([1]-[4], [8], [13]). Author's discrete form of this theorem states that for each $X, Y \in \mathbb{R}^n$ ($n \geq 2$) at algebraic distance there exists a finite set S_{XY} with $\{X, Y\} \subseteq S_{XY} \subseteq \mathbb{R}^n$ such that each unit-distance preserving mapping $g : S_{XY} \to \mathbb{R}^n$ satisfies $|X - Y| = |g(X) - g(Y)|$ ([18], [19]).

Case 1: $r \in \mathbb{R}^{\mathrm{alg}}$ and $r \geq 0$.

The points $X = (0, 0) \in \mathbb{R}^2$ and $Y = (\sqrt{r}, 0) \in \mathbb{R}^2$ are at algebraic distance $\sqrt{r}$. We consider the finite set $S_{XY} = \{(x_1, y_1), ..., (x_n, y_n)\}$ that exists by the discrete form of the Beckman-Quarles theorem. We prove that

$$\begin{aligned} A(r) = \{0,\ 1,\ r,\ \sqrt{r}\} \cup \{x_i :\ \ 1 \leq i \leq n\} \cup \{y_i :\ \ 1 \leq i \leq n\} \ \ \cup \\ \{x_i - x_j :\ \ 1 \leq i \leq n,\ \ 1 \leq j \leq n\} \cup \{y_i - y_j :\ \ 1 \leq i \leq n,\ \ 1 \leq j \leq n\} \ \ \cup \\ \{(x_i - x_j)^2 :\ \ 1 \leq i \leq n,\ \ 1 \leq j \leq n\} \cup \{(y_i - y_j)^2 :\ \ 1 \leq i \leq n,\ \ 1 \leq j \leq n\} \end{aligned}$$

is adequate for r. Assume that $f : A(r) \to \mathbb{R}$ satisfies conditions **(1)**-**(3)**. We show that $(f, f) : S_{XY} \to \mathbb{R}^2$ preserves unit distance. Assume that $|(x_i, y_i) - (x_j, y_j)| = 1$, where $1 \leq i \leq n,\ \ 1 \leq j \leq n$. Then $(x_i - x_j)^2 + (y_i - y_j)^2 = 1$ and

$$\begin{aligned} 1 = f(1) &= \\ f((x_i - x_j)^2 + (y_i - y_j)^2) &= \\ f((x_i - x_j)^2) + f((y_i - y_j)^2) &= \\ (f(x_i - x_j))^2 + (f(y_i - y_j))^2 &= \\ (f(x_i) - f(x_j))^2 + (f(y_i) - f(y_j))^2 &= |(f, f)(x_i, y_i) - (f, f)(x_j, y_j)|^2. \end{aligned}$$

Therefore, $|(f, f)(x_i, y_i) - (f, f)(x_j, y_j)| = 1$. By the property of S_{XY} $|X - Y| = |(f, f)(X) - (f, f)(Y)|$. Therefore, $(0 - \sqrt{r})^2 + (0 - 0)^2 = |X - Y|^2 = |(f, f)(X) -$

$(f,f)(Y)|^2 = (f(0) - f(\sqrt{r}))^2 + (f(0) - f(0))^2$. Since $f(0) = 0$, we have $r = (f(\sqrt{r}))^2$. Thus $f(\sqrt{r}) = \pm\sqrt{r}$. It implies $f(r) = f(\sqrt{r} \cdot \sqrt{r}) = (f(\sqrt{r}))^2 = r$.

CASE 2: $r \in \mathbb{R}^{\mathrm{alg}}$ and $r < 0$.

By the proof for case 1 there exists $A(-r)$ that is adequate for $-r$. We prove that $A(r) = \{0,\ r\} \cup A(-r)$ is adequate for r. Assume that $f : A(r) \to \mathbb{R}$ satisfies conditions **(1)**-**(3)**. Then $f_{|A(-r)} : A(-r) \to \mathbb{R}$ satisfies conditions **(1)**-**(3)** defined for $A(-r)$ instead of $A(r)$. Hence $f(-r) = -r$. Since $0 = f(0) = f(r + (-r)) = f(r) + f(-r) = f(r) - r$, we conclude that $f(r) = r$.

We prove:

(7) if $r \in \widetilde{\mathbb{R}}$ then $r \in \mathbb{R}^{\mathrm{alg}}$.

Let $r \in \widetilde{\mathbb{R}}$ and some $A(r) = \{r = x_1, ..., x_n\}$ is adequate for r. Let also $x_i \neq x_j$ if $i \neq j$. We choose all formulae $x_i = 1$ $(1 \leq i \leq n)$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$ $(1 \leq i \leq j \leq n$, $1 \leq k \leq n)$ that are satisfied in $A(r)$. Joining these formulae with conjunctions we get some formula Φ. Let V denote the set of variables in Φ, $x_1 \in V$ since otherwise for any $s \in \mathbb{R} \setminus \{r\}$ the mapping $f = \mathrm{id}(A(r) \setminus \{r\}) \cup \{(r,s)\}$ satisfies conditions **(1)**-**(3)** and $f(r) \neq r$. Analogously as in the proof of Theorem 2:

(8) the formula $\underbrace{...\ \exists x_i\ ...}_{x_i \in V,\ i \neq 1}\ \Phi$ is satisfied in $\mathbb{R}$ if and only if $x_1 = r$.

The theory of real closed fields is model complete ([7, THEOREM 8.6, p. 130]). The fields $\mathbb{R}$ and $\mathbb{R}^{\mathrm{alg}}$ are real closed. Hence $\mathrm{Th}(\mathbb{R}) = \mathrm{Th}(\mathbb{R}^{\mathrm{alg}})$. By this, the sentence $\underbrace{...\ \exists x_i\ ...}_{x_i \in V} \Phi$ which is true in $\mathbb{R}$, is also true in $\mathbb{R}^{\mathrm{alg}}$. Therefore, for indices i with $x_i \in V$ there exist $w_i \in \mathbb{R}^{\mathrm{alg}}$ such that $\mathbb{R}^{\mathrm{alg}} \models \Phi[x_i \mapsto w_i]$. Since Φ is quantifier free, $\mathbb{R} \models \Phi[x_i \mapsto w_i]$. Thus, by **(8)** $w_1 = r$, so $r \in \mathbb{R}^{\mathrm{alg}}$.

Remark 2. Similarly to **(7)** the discrete form of the Beckman-Quarles theorem does not hold for any $X, Y \in \mathbb{R}^n$ $(n \geq 2)$ at non-algebraic distance ([18]).

Remark 3. A well-known result:

if $f : \mathbb{R} \to \mathbb{R}$ is a field homomorphism, then $f = \mathrm{id}(\mathbb{R})$ ([10]-[12])

may be proved geometrically as follows. If $f : \mathbb{R} \to \mathbb{R}$ is a field homomorphism then $(f,f) : \mathbb{R}^2 \to \mathbb{R}^2$ preserves unit distance; we prove it analogously as in **(III)**. By the classical Beckman-Quarles theorem (f,f) is an isometry. Since the isometry (f,f) has three non-collinear fixed points: $(0,0)$, $(1,0)$, $(0,1)$, we conclude that $(f,f) = \mathrm{id}(\mathbb{R}^2)$ and $f = \mathrm{id}(\mathbb{R})$.

2. A discrete form of the theorem that each field endomorphism of $\mathbb{Q}_p$ is the identity

Let $\mathbb{Q}_p$ be the field of p-adic numbers, $|\cdot|_p$ denote the p-adic norm on $\mathbb{Q}_p$, $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. Let $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ denote the valuation function written additively: $v_p(x) = -\log_p(|x|_p)$ if $x \neq 0$, $v_p(0) = \infty$. For $n \in \mathbb{Z}$, $a, b \in \mathbb{Q}_p$ by

$a \equiv b \pmod{p^n}$ we understand $|a-b|_p \le p^{-n}$. It is known ([11],[16],[22]) that each field automorphism of $\mathbb{Q}_p$ is the identity.

Lemma 1 (Hensel's lemma, [9]). Let $F(x) = c_0 + c_1 x + \ldots + c_n x^n \in \mathbb{Z}_p[x]$. Let $F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \ldots + nc_n x^{n-1}$ be the formal derivative of $F(x)$. Let $a_0 \in \mathbb{Z}_p$ such that $F(a_0) \equiv 0 \pmod{p}$ and $F'(a_0) \not\equiv 0 \pmod{p}$. Then there exists a unique $a \in \mathbb{Z}_p$ such that $F(a) = 0$ and $a \equiv a_0 \pmod{p}$.

Lemma 2 ([6]). For each $x \in \mathbb{Q}_p$ $(p \neq 2)$ $|x|_p \le 1$ if and only if there exists $y \in \mathbb{Q}_p$ such that $1 + px^2 = y^2$. For each $x \in \mathbb{Q}_2$ $|x|_2 \le 1$ if and only if there exists $y \in \mathbb{Q}_2$ such that $1 + 2x^3 = y^3$.

Proof in case $p \neq 2$. If $|x|_p \le 1$ then $v_p(x) \ge 0$ and $x \in \mathbb{Z}_p$. We apply Lemma 1 for $F(y) = y^2 - 1 - px^2$ and $a_0 = 1$. This a_0 satisfies the assumptions: $F(a_0) = -px^2 \equiv 0 \pmod{p}$ and $F'(a_0) = 2 \not\equiv 0 \pmod{p}$. By Lemma 1 there exists $y \in \mathbb{Z}_p$ such that $F(y) = 0$, so $1 + px^2 = y^2$. If $|x|_p > 1$ then $v_p(x) < 0$. By this $v_p(1+px^2) = v_p(px^2) = 1 + 2v_p(x)$ is not divisible by 2, so $1 + px^2$ is not a square.

Proof in case $p = 2$. If $|x|_2 \le 1$ then $v_2(x) \ge 0$ and $x \in \mathbb{Z}_2$. We apply Lemma 1 for $F(y) = y^3 - 1 - 2x^3$ and $a_0 = 1$. This a_0 satisfies the assumptions: $F(a_0) = -2x^3 \equiv 0 \pmod{2}$ and $F'(a_0) = 3 \not\equiv 0 \pmod{2}$. By Lemma 1 there exists $y \in \mathbb{Z}_2$ such that $F(y) = 0$, so $1 + 2x^3 = y^3$. If $|x|_2 > 1$ then $v_2(x) < 0$. By this $v_2(1+2x^3) = v_2(2x^3) = 1 + 3v_2(x)$ is not divisible by 3, so $1 + 2x^3$ is not a cube.

Lemma 3. If $c, d \in \mathbb{Q}_p$ and $c \neq d$, then there exist $m \in \mathbb{Z}$ and $u \in \mathbb{Q}$ such that $|\frac{c-u}{p^{m+1}}|_p \le 1$ and $|\frac{d-u}{p^{m+1}}|_p > 1$.

Proof. Let $c = \sum\limits_{k=s}^{\infty} c_k p^k$ and $d = \sum\limits_{k=s}^{\infty} d_k p^k$, where $s \in \mathbb{Z}$, $c_k, d_k \in \{0, 1, \ldots, p-1\}$. Then $m = \min\{k : c_k \neq d_k\}$ and $u = \sum\limits_{k=s}^{m} c_k p^k$ satisfy our conditions.

Let $\mathbb{Q}_p^{\text{alg}} = \{x \in \mathbb{Q}_p : x \text{ is algebraic over } \mathbb{Q}\}$.

Theorem 7. $\widetilde{\mathbb{Q}_p} = \mathbb{Q}_p^{\text{alg}}$.

Proof. We prove: if $r \in \mathbb{Q}_p^{\text{alg}}$ then $r \in \widetilde{\mathbb{Q}_p}$.

Let $r \in \mathbb{Q}_p^{\text{alg}}$. Since $r \in \mathbb{Q}_p$ is algebraic over $\mathbb{Q}$, it is a zero of a polynomial $p(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $a_n \neq 0$. Let $R = \{r = r_1, r_2, \ldots, r_k\}$ be the set of all roots of $p(x)$ in $\mathbb{Q}_p$. For each $j \in \{2, 3, \ldots, k\}$ we apply Lemma 3 for $c = r$ and $d = r_j$ and choose $m_j \in \mathbb{Z}$ and $u_j \in \mathbb{Q}$ such that $|\frac{r-u_j}{p^{m_j+1}}|_p \le 1$ and $|\frac{r_j-u_j}{p^{m_j+1}}|_p > 1$. Let $u_j = \frac{s_j}{t_j}$, where $s_j \in \mathbb{Z}$ and $t_j \in \mathbb{Z} \setminus \{0\}$. In case $p \neq 2$ by Lemma 2 for each $j \in \{2, 3, \ldots, k\}$ there exists $y_j \in \mathbb{Q}_p$ such that

$$1 + p\left(\frac{r - u_j}{p^{m_j+1}}\right)^2 = y_j^2.$$

In case $p=2$ by Lemma 2 for each $j \in \{2,3,...,k\}$ there exists $y_j \in \mathbb{Q}_2$ such that

$$1+2\biggl(\frac{r-u_j}{2^{m_j+1}}\biggr)^3 = y_j^3.$$

Let $a = \max\ \{p, |a_i|, |s_j|, |t_j|, |m_j+1|:\ 0 \le i \le n,\ 2 \le j \le k\}$. The set

$$A(r) = \{\sum_{i=0}^{n} b_i r^i : b_i \in \mathbb{Z} \cap [-a,a]\} \cup \{p^w :\ w \in \mathbb{Z} \cap [-a,a]\} \cup$$

$$\bigcup_{j=2}^{k} \{u_j,\ r-u_j,\ \tfrac{r-u_j}{p^{m_j+1}},\ \left(\tfrac{r-u_j}{p^{m_j+1}}\right)^2,\ p\left(\tfrac{r-u_j}{p^{m_j+1}}\right)^2,\ \left(\tfrac{r-u_j}{p^{m_j+1}}\right)^3,\ p\left(\tfrac{r-u_j}{p^{m_j+1}}\right)^3,\ y_j,\ y_j^2,\ y_j^3\}$$

is finite, $r \in A(r)$. We prove that $A(r)$ is adequate for r. Assume that $f : A(r) \to \mathbb{Q}_p$ satisfies conditions **(1)**-**(3)**. Analogously as in **(I)** we conclude that $f(r) = r_j$ for some $j \in \{1,2,...,k\}$. Therefore, $f(r) = r$ if $k = 1$. Let $k \ge 2$. Suppose, on the contrary, that

$(*)$ $$f(r) = r_j \text{ for some } j \in \{2,3,...,k\}.$$

In case $p \ne 2$ supposition $(*)$ implies:

$$1+p\biggl(\frac{r_j-u_j}{p^{m_j+1}}\biggr)^2 = 1+p\biggl(\frac{f(r)-u_j}{p^{m_j+1}}\biggr)^2 = f\left(1+p\biggl(\frac{r-u_j}{p^{m_j+1}}\biggr)^2\right) = f(y_j^2) = f(y_j)^2.$$

Thus, by Lemma 2 $\left|\frac{r_j-u_j}{p^{m_j+1}}\right|_p \le 1$, a contradiction. In case $p=2$ supposition $(*)$ implies:

$$1+2\biggl(\frac{r_j-u_j}{2^{m_j+1}}\biggr)^3 = 1+2\biggl(\frac{f(r)-u_j}{2^{m_j+1}}\biggr)^3 = f\left(1+2\biggl(\frac{r-u_j}{2^{m_j+1}}\biggr)^3\right) = f(y_j^3) = f(y_j)^3.$$

Thus, by Lemma 2 $\left|\frac{r_j-u_j}{2^{m_j+1}}\right|_2 \le 1$, a contradiction.

We prove: if $r \in \widetilde{\mathbb{Q}_p}$ then $r \in \mathbb{Q}_p^{\mathrm{alg}}$.

Let $r \in \widetilde{\mathbb{Q}_p}$ and some $A(r) = \{r = x_1, ..., x_n\}$ is adequate for r. Let also $x_i \ne x_j$ if $i \ne j$. Analogously as in the proof of **(7)** we construct a quantifier free formula Φ such that

(9) the formula $\underbrace{...\ \exists x_i\ ...}_{x_i \in V,\ i \ne 1}\ \Phi$ is satisfied in $\mathbb{Q}_p$ if and only if $x_1 = r$;

as previously, V denote the set of variables in Φ and $x_1 \in V$. $\mathrm{Th}(\mathbb{Q}_p) = \mathrm{Th}(\mathbb{Q}_p^{\mathrm{alg}})$, it follows from the first sentence on page 134 in [15], see also [14, Theorem 10, p. 151]. By this, the sentence $\underbrace{...\ \exists x_i\ ...}_{x_i \in V}\Phi$ which is true in $\mathbb{Q}_p$, is also true in $\mathbb{Q}_p^{\mathrm{alg}}$. Therefore,

for indices i with $x_i \in V$ there exist $w_i \in \mathbb{Q}_p^{\rm alg}$ such that $\mathbb{Q}_p^{\rm alg} \models \Phi[x_i \mapsto w_i]$. Since Φ is quantifier free, $\mathbb{Q}_p \models \Phi[x_i \mapsto w_i]$. Thus, by **(9)** $w_1 = r$, so $r \in \mathbb{Q}_p^{\rm alg}$.

3. Applying R. M. Robinson's theorem on definability

Let a field $\boldsymbol{K}$ extends $\mathbb{Q}$ and each element of $\boldsymbol{K}$ is algebraic over $\mathbb{Q}$. R. M. Robinson proved ([17]): if $r \in \boldsymbol{K}$ is fixed for all automorphisms of $\boldsymbol{K}$, then there exist $U(y), V(y) \in \mathbb{Q}[y]$ such that $\{r\}$ is definable in $\boldsymbol{K}$ by the formula $\exists y\ (U(y) = 0 \wedge x = V(y))$. By Robinson's theorem $\widetilde{\mathbb{R}^{\rm alg}} = \mathbb{R}^{\rm alg}$ and $\widetilde{\mathbb{Q}_p^{\rm alg}} = \mathbb{Q}_p^{\rm alg}$. Since $\mathbb{R}^{\rm alg}$ is an elementary subfield of $\mathbb{R}$ ([7]), $\widetilde{\mathbb{R}} = \widetilde{\mathbb{R}^{\rm alg}}$, and finally $\widetilde{\mathbb{R}} = \mathbb{R}^{\rm alg}$. Since $\mathbb{Q}_p^{\rm alg}$ is an elementary subfield of $\mathbb{Q}_p$ ([14],[15]), $\widetilde{\mathbb{Q}_p} = \widetilde{\mathbb{Q}_p^{\rm alg}}$, and finally $\widetilde{\mathbb{Q}_p} = \mathbb{Q}_p^{\rm alg}$.

Acknowledgement. The author thanks the anonymous referee for valuable suggestions.

References

[1] F. S. Beckman and D. A. Quarles Jr., *On isometries of euclidean spaces*, Proc. Amer. Math. Soc. 4 (1953), 810–815.

[2] W. Benz, *An elementary proof of the theorem of Beckman and Quarles*, Elem. Math. 42 (1987), 4–9.

[3] W. Benz, *Geometrische Transformationen (unter besonderer Berücksichtigung der Lorentztransformationen)*, BI Wissenschaftsverlag, Mannheim, 1992.

[4] W. Benz, *Real geometries*, BI Wissenschaftsverlag, Mannheim, 1994.

[5] M. Davis, Y. Matijasevič and J. Robinson, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution*, in: Mathematical developments arising from Hilbert problems (ed. F. E. Browder), Proc. Sympos. Pure Math., vol. 28, Part 2, Amer. Math. Soc., 1976, 323–378; reprinted in: The collected works of Julia Robinson (ed. S. Feferman), Amer. Math. Soc., 1996, 269–324.

[6] F. Delon, *Some p-adic model theory*, in: European Women in Mathematics: Proceedings of the 8th General Meeting (ed. L. Fainsilber and C. Hobbs), Hindawi Publishing Corporation, Stony Brook, 1999, 63–76.

[7] P. C. Eklof, *Ultraproducts for algebraists*, in: Handbook of mathematical logic (ed. J. Barwise), North-Holland, Amsterdam, 1977, 105–137.

[8] U. Everling, *Solution of the isometry problem stated by K. Ciesielski*, Math. Intelligencer 10 (1988), No. 4, p. 47.

[9] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Springer-Verlag, New York, 1977.

[10] M. Kuczma, *An introduction to the theory of functional equations and inequalities: Cauchy's equation and Jensen's inequality*, Polish Scientific Publishers and Silesian University, Warszawa-Kraków-Katowice, 1985.

[11] S. Lang, *Algebra*, 2nd ed., Addison-Wesley, Menlo Park, California, 1984.

[12] J. Lelong-Ferrand, *Les fondements de la géométrie*, Presses Universitaires de France, Paris, 1985.

[13] J. A. Lester, *Distance preserving transformations*, in: Handbook of incidence geometry (ed. F. Buekenhout), North-Holland, Amsterdam, 1995, 921–944.

[14] A. MacIntyre, *Model completeness*, in: Handbook of mathematical logic (ed. J. Barwise), North-Holland, Amsterdam, 1977, 139–180.

[15] A. MacIntyre, *Twenty years of p-adic model theory*, in: Logic Colloquium '84 (eds. J. B. Paris, A. J. Wilkie, G. M. Wilmers), North-Holland, Amsterdam, 1986, 121–153.

[16] A. M. Robert, *A course in p-adic analysis*, Springer-Verlag, New York, 2000.

[17] R. M. Robinson, *Arithmetical definability of field elements*, J. Symbolic Logic 16 (1951), 125–126.

[18] A. Tyszka, *Discrete versions of the Beckman-Quarles theorem*, Aequationes Math. 59 (2000), 124–133.

[19] A. Tyszka, *Discrete versions of the Beckman-Quarles theorem from the definability results of R. M. Robinson*, Algebra, Geometry & their Applications, Seminar Proceedings 1 (2001), 88–90, Yerevan State University Press.

[20] A. Tyszka, *Beckman-Quarles type theorems for mappings from* $\mathbb{R}^n$ *to* $\mathbb{C}^n$, Aequationes Math. 67 (2004), 225–235.

[21] A. Tyszka, *Existentially* $\emptyset$*-definable elements in a field*, http://arxiv.org/abs/math.LO/0502565

[22] C. G. Wagner, *Automorphisms of p-adic number fields*, Amer. Math. Monthly 81 (1974), 51–52.

Apoloniusz Tyszka
Technical Faculty
Hugo Kołłątaj University
Balicka 104, 30-149 Kraków, Poland
E-mail address: *rttyszka@cyf-kr.edu.pl*